

KB 150183

IDENTIKEY Authentication Server rejects the authentication with the message "RADIUS requests are disallowed in the policy protocol list, request will be rejected."

Creation date: 07/07/2017

Last Review: 11/09/2017

Revision number: 2

Document type: How To

Security status: EXTERNAL

Summary

When trying a RADIUS Authentication, you get the following error in the trace file: "RADIUS requests are disallowed in the policy protocol list, request will be rejected"

This document describes the reason for this error and how to solve it.

Problem details.

In the trace file you see the following:

```
[2017/07/06|15:59:10.002513UTC][S0/P4636/T01912][VINFO][CUDPSocket::recvfrom] > Packet received from <192.168.20.110 : 54169> size <103> bytes.
```

...

```
[2017/07/06|15:59:10.008514UTC][S0/P4636/T01600][DEBUG][ComponentLoader::fetchComponent] > Existing Component record [RADIUS Client:default] returned from Component Cache
```

...

```
[2017/07/06|15:59:10.034517UTC][S0/P4636/T01600][VINFO][RADIUSLayer::dispatchCommandTask] > Authentication request received.
```

```
[2017/07/06|15:59:10.034517UTC][S0/P4636/T01600][VINFO][RADIUSLayer::dispatchCommandTask] > PAP RADIUS requests are disallowed in the policy protocol list, request will be rejected.
```

```
[2017/07/06|15:59:10.035517UTC][S0/P4636/T01600][INFO][ad_record] > Audit: {Info} {RADIUS} {I-007003} {A RADIUS Access-Reject has been issued.}
```

Problem Solution.

This error is due to the configuration of the Policy connected to the RADIUS client used (in the above example the RADIUS Client:default is used)

In the policy there is a tab RADIUS, and an Item Supported Protocols.
By default this is set to any.

Applies to: IDENTIKEY Authentication Server

KB 150183- 11/09/2017

© 2017 VASCO Data Security. All rights reserved.

Page 1 of 2

Manage policy: Identikey Local Authentication
Click on the tabs to view or change policy settings.

Policy User DIGIPASS Challenge Secure Channel Virtual DIGIPASS DP Control Parameters

Offline Authentication Password Randomization DCR **RADIUS**

Available Actions... [Click here to close and return to previous page](#)

Effective Settings

RADIUS Protocol Settings

Supported Protocols	Default	(Any)
Wireless Session Lifetime	Default (seconds)	(3600)

TLS Session Settings

TLS Session Lifetime	Default (seconds)	(86400)
Maximum Fast Reconnect Count	Default (reuses)	(48)

If this setting is changed, and some Radius Protocols are excluded you will have this issue when using the excluded protocol.

Eg when the PAP protocol is excluded:

Manage policy: TestRad
Click on the tabs to view or change policy settings.

Policy User DIGIPASS Challenge Secure Channel Virtual DIGIPASS DP Control Parameters

Offline Authentication Password Randomization DCR **RADIUS**

Edit RADIUS Settings

Current Effective Settings

RADIUS Protocol Settings

Supported Protocols

Custom

- EAP-TTLS
- PEAPv1
- PEAPv0
- PAP
- CHAP
- MSCHAP
- MSCHAP2
- VASCO-Specific

Wireless Session Lifetime (seconds) (3600)

(EAP-TTLS, PEAPv1, PEAPv0, CHAP, MSCHAP, MSCHAP2, VASCO-Specific)

And you try to make a RADIUS Authentication with the PAP protocol, you will see the error as in the example above.